Grant Thornton

Services financiers Perspectives en matière de réglementation

2024-2025

Sommaire

Introduction	**03**
Comment pouvons-nous vous aider ?	**03**
Nouveaux développements prudentiels	**04**
Résilience opérationnelle	**08**
Digitalisation et utilisation de l'IA dans la finance	**13**

Introduction

Les évolutions réglementaires en cours au sein de l'Union européenne contribuent à façonner de manière durable l'industrie financière européenne, sa stabilité et influent sur les stratégies des différents acteurs financiers.
Les acteurs (banques, compagnies d'assurance…) sont ainsi appelés à naviguer dans des eaux troubles et remplies d'incertitudes (allant de l'évolution des facteurs géopolitiques aux technologies émergentes) et devront mettre en œuvre les changements nécessaires induits par ces évolutions réglementaires.

L'objectif des régulateurs à travers ces différents textes vise d'une part, à renforcer la stabilité des institutions financières au sein de l'UE, d'autre part à protéger les consommateurs.
Malgré cette inflation de textes réglementaires, qui affectent leurs opérations et leurs stratégies, les institutions financières devront se conformer à ces réglementations.
Cette publication présente les principales évolutions du paysage réglementaire de l'UE impactant le secteur financier, et explore les principales incertitudes qui peuvent influer sur les processus de prise de décision.

Azarias Sekko

Comment pouvons-nous vous aider ?

Pour naviguer dans le paysage complexe des réglementations de l'UE, il faut avoir une compréhension nuancée d'un cadre juridique en constante évolution, rester au fait des mises à jour réglementaires, favoriser la collaboration avec les organismes de réglementation et tirer parti des avancées technologiques.

Chez Grant Thornton, nous pouvons accompagner votre établissement dans le cadre de l'adoption des différentes réglementations et garantir l'adaptabilité avec une approche proactive. Nos services sont assurés par des experts en la matière, à la pointe de leur domaine. Nous travaillerons avec vous pour nous assurer que la mise en œuvre requise, complète votre stratégie commerciale globale et garantit la conformité.

<u>Nos experts en services financiers (banque, gestion d'actifs) :</u>

Azarias Sekko
Associé, Audit
M azarias.sekko@fr.gt.com
T +33 1 41 25 90 67

Leslie Fitoussi
Directrice Associée, Audit
M leslie.fitoussi@fr.gt.com
T +33 1 41 25 87 39

Didier Alleaume
Associé, Conseil
M didier.alleaume@fr.gt.com
T +33 1 41 25 93 61

Céline Roy Larentry
Directrice Associée, Conseil
M celine.roy-larentry@fr.gt.com
T +33 1 41 25 96 33

Frédéric Gaulier
Associé, *Outsourcing*
M frederic.gaulier@fr.gt.com
T +33 1 41 25 87 59

Gilles Verny
Directeur Associé, *Outsourcing*
M gilles.verny@fr.gt.com
T +33 1 41 25 94 88

Alexis Grin
Associé, *IT*
M alexis.grin@fr.gt.com
T +33 1 41 25 91 64

<u>Autres experts :</u>
Franco Tortato, Directeur, *Financial Services Outsourcing*,
Abdel Farid Ale, Directeur, Cybersécurité

Nouveaux développements prudentiels

Adoption du nouveau paquet bancaire - (CRR III / CRD VI)

Le paquet bancaire modifie la directive 2013/36/UE (directive CRD) et le règlement (UE) N° 575/2013 (règlement CRR).

Le paquet bancaire met en œuvre, dans l'Union européenne, le dernier volet de la réforme réglementaire de Bâle III (à savoir le plancher de fonds propres, le risque de crédit, le risque de marché et le risque opérationnel). Il introduit également des changements dans d'autres domaines-clés ne relevant pas des accords de Bâle tels que l'honorabilité, les succursales de pays tiers et les risques environnementaux, sociaux et de gouvernance (dits « ESG »).

Dans le cadre du paquet bancaire, l'EBA a reçu différents mandats en vue d'élaborer de nouvelles dispositions réglementaires telles que des normes techniques d'exécution *Implementation Technical Standards (ITS)* / des normes techniques de réglementation *Regulatory Technical Standards (RTS)* et des orientations afin de renforcer le cadre de surveillance, d'apporter des éclaircissements à l'industrie et, enfin, de garantir des conditions équitables *(level playing field)*.

Le règlement CRR III et la directive CRD VI sont entrés en vigueur le **9 juillet 2024**.

Le règlement CRR III sera en général applicable à compter du **1er janvier 2025** (certaines dispositions étant déjà en vigueur à compter du 9 juillet 2024). Certaines dispositions du règlement CRR III sont également soumises à des dispositions transitoires et entreront progressivement en vigueur dans les années à venir. En ce qui concerne les règles relatives aux risques de marché et la revue fondamentale du portefeuille de marché *(Fundamental Review of the Trading Book, FRTB)*, la Commission européenne a annoncé le 18 juin 2024 que leur date d'application dans l'UE avait été reportée d'un an au **1er janvier 2026**. Ce report sera adopté par acte délégué plus tard cette année.

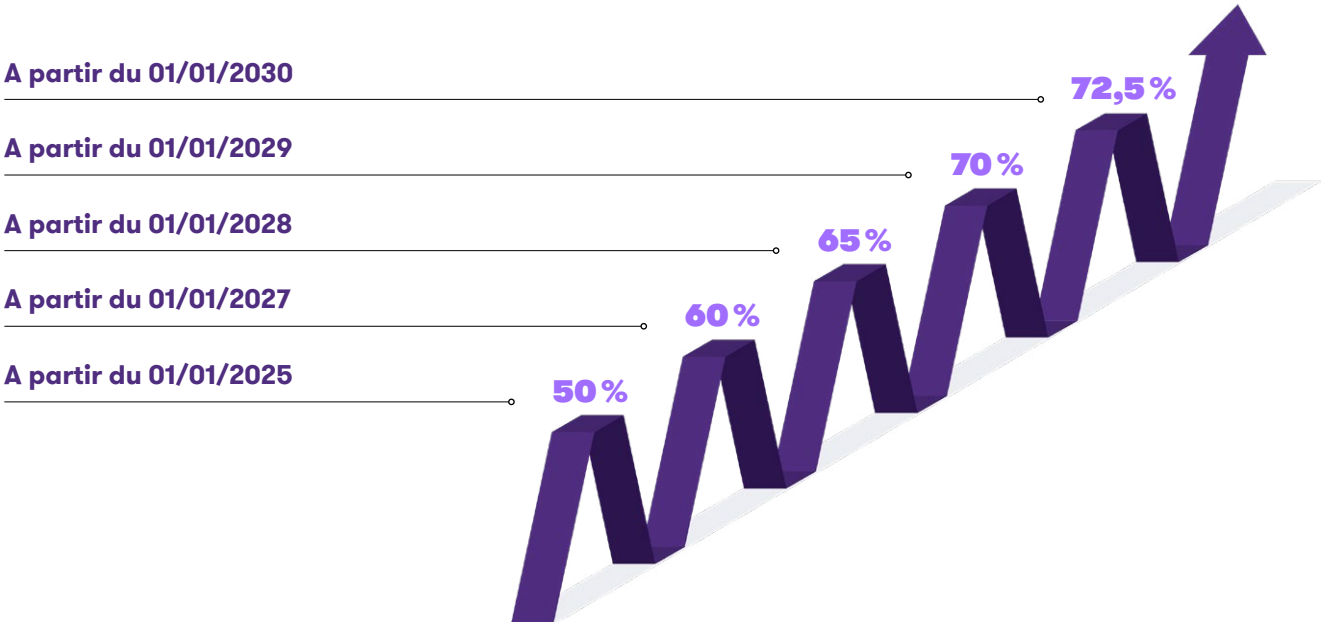
La directive CRD VI devra être transposée par les États membres en droit national au plus tard le **10 janvier 2026**. En général, elle sera applicable à compter du **11 janvier 2026**, à l'exception des dispositions sur les succursales de pays tiers qui seront applicables un an plus tard, à compter du **11 janvier 2027**.

Les principales évolutions introduites par CRR3

Le nouveau règlement vise à renforcer la résilience du système bancaire et sa capacité à soutenir l'économie réelle. Il a notamment de nombreux impacts sur le risque de crédit et le risque opérationnel, dont voici les principaux :

› Introduction d'un *Outpoot Floor*

Le règlement CRR3 introduit la mise en place de *outpoot floor* ou plancher en capital, qui a pour objectif de limiter le bénéfice que les institutions financières pourraient tirer de l'utilisation des modèles internes. Cette mesure vise à garantir que les résultats des modèles internes conduisent à des niveaux suffisants de fonds propres pour couvrir les pertes potentielles. Le plancher est fixé en pourcentage des actifs pondérés en fonction du risque calculé selon l'approche standardisée et est progressivement mis en place sur une période de transition s'étalant de 2025 à 2032.



Révision de l'approche standard

Le règlement CRR3 vise à rendre l'approche standard plus sensible au risque, en ajoutant notamment plus de granularité dans les classes d'expositions spécifiques et en révisant les pondérations de risque prudentiel. Ainsi :

- Pour les expositions garanties par des actifs immobiliers, des distinctions ont été ajoutées en fonction du type de financement de l'exposition (selon qu'il dépend ou non des revenus générés par le bien immobilier) et du stade de développement du bien (en construction ou terminé). Le ratio Exposition-Valeur (ETV) a été modifié en conséquence pour les prêts hypothécaires résidentiels et commerciaux,
- L'exigence de multiplicateur de pondération de risque a été introduite pour les expositions immobilières résidentielles non couvertes par des instruments de couverture,
- La pondération du risque pour les expositions aux institutions sans évaluation de crédit par une Institution Nominée d'Évaluation du Crédit Externe (ECAI) a été révisée pour s'aligner sur Bâle III. Cette méthode implique de classer les expositions en trois catégories selon des critères quantitatifs et qualitatifs, avec des exigences supplémentaires en matière de diligence raisonnable.

Révision de l'approche *IRB*

Le nouveau règlement introduit une réduction de la portée des expositions éligibles aux modèles *IRB (Internal Rating-Based)* pour le risque de crédit. En effet, comme la commission européenne vise à accroître l'harmonisation entre les institutions et à rendre les résultats des modèles *IRB* plus comparables, le cadre *IRB* a été révisé. Ainsi, le règlement CRR3 limite l'utilisation de l'approche *Advanced IRB (A-IRB)* uniquement aux classes d'exposition où une modélisation robuste est jugée réalisable (par exemple, les expositions aux grandes entreprises ou aux institutions) - tandis que d'autres classes d'exposition seront migrées vers des méthodes moins sophistiquées (c'est-à-dire, sous la méthode *Foundation IRB (F-IRB)* ou méthode standard).

De plus, les expositions aux entités du secteur public, aux gouvernements régionaux et aux autorités locales seront traitées dans une nouvelle classe d'exposition « PSE-RGLA » et seront soumises aux mêmes exigences que le régime d'exposition général aux entreprises.

Enfin, des planchers d'entrée seront introduits pour établir des niveaux minimaux d'estimations propres (c'est-à-dire, Probabilité de Défaut (PD), *Loss Given Default (LGD)*, *Exposure At Default (EAD)*) dans le cadre *IRB*. Les expositions souveraines seront cependant exemptées de l'application des nouveaux planchers d'entrée.

Cadre opérationnel

Le cadre actuel de risque opérationnel sera remplacé par une nouvelle approche standardisée pour les exigences en fonds propres couvrant les incidents opérationnels. L'Approche de Mesure Avancée (AMA), qui permettait l'utilisation de modèles statistiques internes, sera donc supprimée.

Cette nouvelle approche standardisée repose sur une mesure comptable basée sur les revenus de la banque (composante de l'indicateur d'activité) et l'expérience des pertes historiques (multiplicateur des pertes internes). Elle suppose que le risque opérationnel augmente à un taux croissant en fonction des revenus de la banque et que la probabilité d'occurrence de pertes liées au risque opérationnel augmente si la banque a enregistré des pertes historiques plus élevées dans ce domaine.

Les principales évolutions introduites par CRD VI

La directive CRD6 introduit plusieurs évolutions importantes sur des enjeux non liés à la mise en œuvre de Bâle 3, afin d'harmoniser différents bouts de la réglementation prudentielle et de mieux inclure les risques émergents dans le cadre de supervision. Voici-ci-dessous les principales évolutions qui impacteront les banques :

› Renforcement de l'intégration des risques ESG

Le package réglementaire introduit des changements significatifs pour intégrer les risques environnementaux, sociaux et de gouvernance (ESG) dans les trois piliers de la réglementation bancaire. Au premier pilier, l'EBA est chargée de proposer des méthodes d'évaluation des risques environnementaux à différentes échéances. Dans le cadre du pilier 2, une révision importante est prévue, intégrant les risques ESG dans le processus de contrôle prudentiel et exigeant des banques des tests de résistance réguliers liés aux ESG. L'EBA est également mandatée pour élaborer des orientations sur les méthodologies de ces tests. En ce qui concerne le pilier 3, une extension du champ d'application est proposée, exigeant des établissements bancaires qu'ils quantifient leurs expositions aux risques physiques et de transitions.

Ainsi en pratique, une banque qui accordera des financements à des entreprises ne respectant pas les objectifs de réduction des émissions de carbone, sera exposée à des risques de transition significatifs. Selon la CRD6, cette banque sera tenue de mettre en place une stratégie visant à évaluer et à gérer cette augmentation du risque, tout en accompagnant les clients dans leur transition et leur adaptation.

› Gestion des succursales de pays tiers

La directive introduit notamment un changement significatif en imposant une interdiction aux institutions de pays tiers de fournir des services bancaires de base (notamment, les prêts, les garanties, les engagements et la réception de dépôts) dans l'UE de manière transfrontalière, c'est-à-dire sans présence physique. Ces institutions sont désormais tenues d'établir des succursales dans chaque État membre concerné, ou une filiale de l'UE dûment agréée utilisant le passeport européen.

Après sa publication, une période de transposition de 18 mois sera accordée aux États membres pour intégrer la CRD VI dans leur législation nationale, suivie d'une période de transition supplémentaire de 12 mois pour les dispositions relatives aux succursales de pays tiers. Les nouvelles règles, y compris les licences, devraient donc entrer en vigueur à partir de l'automne 2026, offrant aux institutions concernées le temps nécessaire pour s'adapter et se conformer aux changements réglementaires. Les obligations de déclaration, quant à elles, prendront effet, au plus tôt, 12 mois après la publication.

Autorité Bancaire Européenne - *Stress tests*

La supervision bancaire européenne utilise des tests de résistance (*stress tests*) pour évaluer le niveau de préparation des banques aux chocs financiers et économiques. Les résultats de ces tests permettent aux autorités de surveillance de détecter les vulnérabilités et de les traiter de façon précoce dans le cadre du dialogue prudentiel avec les banques.

› Types de tests de résistance

La Banque centrale européenne (BCE) conduit plusieurs types de tests de résistance.

- Tests de résistance annuels
  - Tests de résistance à l'échelle de l'Union européenne (UE) coordonnés par l'Autorité bancaire européenne (ABE), complétés par le test de résistance de la BCE dans le cadre du processus de contrôle et d'évaluation prudentiels *(Supervisory Review and Evaluation Process, SREP)* ;
  - Tests de résistance thématiques ;
  - Analyses prospectives de la vulnérabilité.
- Tests de résistance dans le cadre des évaluations complètes,
- Tests de résistance à des fins macroprudentielles (centrés sur la stabilité financière et les conséquences à l'échelle du système et non pas sur les différentes banques).

Outre ces tests, des banques ou groupes de banques peuvent également être soumis à des tests de résistance spécifiques.

L'Autorité bancaire européenne (ABE) a publié le 12 novembre 2024 la méthodologie finale, les projets de modèles et le guide pour les compléter dans le cadre du test de résistance bancaire 2025 qui sera réalisé au niveau de l'Union européenne ainsi que les étapes qu'il poursuit.

Selon le communiqué, le stress test débutera formellement en janvier 2025, après la publication des scénarios macroéconomiques. Les résultats devraient être publiés début août 2025.

La méthodologie et les modèles couvrent tous les domaines de risque pertinents et intègrent les commentaires reçus du secteur.

Les entités participantes doivent estimer la progression des facteurs de risque communs, tels que les risques de crédit, de marché, de contrepartie et opérationnels dans un scénario de base et dans un scénario défavorable. Les banques devront ensuite prévoir l'impact de ces scénarios sur les principales sources de revenus.

Les entreprises seront tenues d'utiliser des « paramètres prédéfinis » pour les revenus nets de commissions, les pondérations des risques de titrisation et l'historique des pertes de crédit des expositions souveraines. En revanche, les projections des revenus nets d'intérêts seront centralisées.

L'ABE a averti que les projets de modèles et d'orientations publiés pour le test pourraient nécessiter « quelques ajustements techniques mineurs » avant leur publication finale au moment de son lancement. La méthodologie définit également l'échantillon de banques qui participent à l'exercice.

Résilience opérationnelle

La BCE conclut son test de résistance sur la cyberrésilience

Le test de résistance visait à évaluer comment les banques réagiraient à un incident de cybersécurité grave mais plausible, et comment elles s'en remettraient.

Il a porté sur 109 banques, dont 28 ont fait l'objet de contrôles plus approfondis.

Les résultats sont pris en compte dans le *SREP* 2024 de la BCE.

La Banque centrale européenne (BCE) a conclu le 26 juillet 2024 son test de résistance sur la cyberrésilience, qui visait à évaluer comment les banques réagiraient à un incident de cybersécurité grave mais plausible, et comment elles s'en remettraient. Dans l'ensemble, le test a montré que les banques disposent de cadres de réaction et de rétablissement mais qu'ils restent des axes d'amélioration. Les résultats de ce test alimenteront le processus de contrôle et d'évaluation prudentiels *(Supervisory Review and Evaluation Process, SREP)* 2024 et ont contribué à sensibiliser davantage les banques aux atouts et aux faiblesses de leurs cadres de cyberrésistance.

L'exercice, qui a débuté en janvier 2024, s'articulait autour d'un scénario fictif dans lequel toutes les mesures préventives échouaient tandis qu'une cyberattaque dégradait gravement les bases de données des systèmes centraux de chaque banque. Il s'agissait donc davantage d'observer comment les banques réagiraient à une cyberattaque et s'en remettraient que d'examiner leurs stratégies de prévention en la matière.

Le test de résistance a concerné 109 banques directement supervisées par la BCE. Toutes les banques ont dû répondre à un questionnaire et soumettre des documents à des fins d'analyse par les autorités prudentielles, tandis qu'un échantillon de 28 banques ont fait l'objet de contrôles plus approfondis. Ces dernières ont été invitées à effectuer un test de restauration informatique et à apporter la preuve de son succès. Elles ont en outre reçu la visite des superviseurs. L'échantillon couvrait différents modèles d'activité et implantations géographiques afin de refléter l'ensemble du système bancaire de la zone euro et d'assurer une coordination suffisante avec les autres activités prudentielles.

La BCE entend maintenir sa collaboration avec les banques qu'elle supervise dans le but de renforcer leurs cadres de cyberrésistance. À cette fin, elle continuera d'encourager les banques à poursuivre leurs travaux en vue de se conformer aux attentes prudentielles, notamment en veillant à ce qu'elles disposent de plans adéquats de continuité des activités, de communication et de rétablissement, qui devraient envisager un éventail suffisamment large de scénarios de risques liés à la cybersécurité. Les banques devraient également être en mesure d'atteindre leurs objectifs de rétablissement, d'évaluer correctement leur dépendance à l'égard des prestataires de services informatiques tiers critiques et d'estimer de façon adéquate les pertes directes et indirectes qui résulteraient d'une cyberattaque.

Les conclusions de l'exercice alimenteront le *SREP 2024*, qui évalue les différents profils de risque des banques. Le test de résistance sur la cyberrésilience n'ayant pas porté sur les fonds propres des banques, ses résultats n'auront pas d'incidence sur les recommandations au titre du pilier 2. Les autorités de surveillance ont fourni un retour d'information à chaque banque, auquel elles donneront suite en conséquence. Certaines banques ont déjà commencé à corriger les insuffisances relevées au cours de l'exercice ou déjà prévu d'y remédier.

Le règlement européen 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier *(DORA)* entrera en application le 17 janvier 2025

Les exigences de ce règlement sont rendues applicables, sauf exceptions, à l'ensemble des entités du secteur financier et concernent :

- La gestion du risque informatique ;
- Le *reporting* des incidents ;
- Les tests de résilience ;
- La gestion du risque de tiers porté par les prestataires de services informatiques.

Les objectifs du projet *DORA*

Le projet de réglementation *DORA* a vocation à renforcer la résilience opérationnelle informatique des acteurs financiers en mettant en place un nouveau cadre de gouvernance et de contrôle interne concernant :

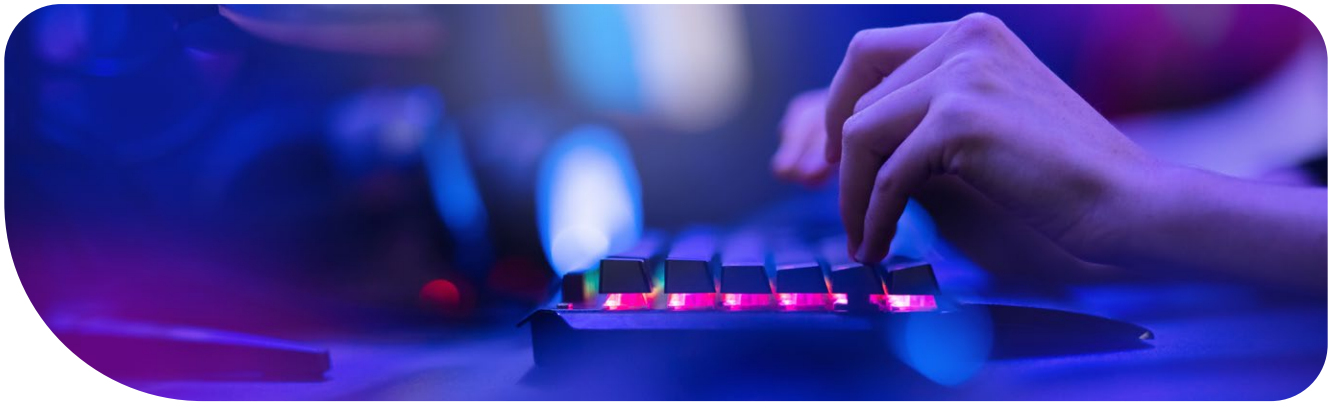
- **La gestion des risques informatiques,**
- **La déclaration des incidents majeurs liés aux technologies,**
- **Les tests de résilience opérationnelle informatique,**
- **La gestion du risque de tiers** avec notamment la supervision directe des prestataires de services « critiques ».

Plus globalement, la directive impose la mise en œuvre d'une stratégie de résilience opérationnelle informatique sous la pleine responsabilité de la direction des institutions financières, dont les principaux objectifs seront :

- **D'améliorer la gestion des incidents liés aux technologies** notamment pour répondre aux exigences de *reporting* vers une instance européenne unique,
- **De renforcer la conduite des tests d'intrusion,**
- **D'étendre le périmètre des plans de continuité aux activités de gestion des technologies** (infrastructures, services informatiques…),
- **S'assurer de la mise en place d'une gestion efficace des risques liés aux technologies.**

L'importance d'une gouvernance forte sous la responsabilité de la Direction est explicitement inscrite dans le projet de règlement (cf. article 4). Ainsi, la Direction doit d'ores et déjà s'assurer de la mise en place d'une gestion efficace des risques liés aux technologies (ICT) se traduisant en particulier par :

- La détermination du niveau de tolérance aux risques liés aux technologies,
- L'approbation, la surveillance et la revue périodique de la politique de continuité des activités et du plan de reprise d'activité liés aux technologies,
- La revue périodique des plans d'audit couvrant les risques informatiques,
- L'approbation et le suivi des contrats d'externalisation de services TIC, notamment en cas de modification des conditions,
- L'allocation et le suivi périodique des budgets pour répondre aux besoins de résilience opérationnelle informatique,
- Le suivi des incidents informatiques et leurs impacts, ainsi que les réponses apportées, les mesures de rétablissement et de correction.



NIS 2

Le 16 janvier 2023 est entrée en vigueur la directive (UE) 2022/2555 du parlement Européen et du Conseil Européen, concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, connue également sous le nom de Directive *NIS 2* « *Network and Information Security* ».

La Directive *NIS 2* **élargit considérablement le champ d'application de la Directive *NIS* de 2016 transposée en France en 2018**. Elle s'adresse à un éventail plus large d'industries pour étendre et renforcer les exigences en matière de cybersécurité dans l'UE.

Ceci inclut la **maîtrise des risques liés au tiers, la rationalisation des obligations de signalement et l'introduction d'exigences strictes en matière de mise en application**. En d'autres termes, la directive *NIS 2* impose à un grand nombre d'organisations de mettre en place un cadre complet de gestion des risques, dans le but d'accroître le niveau global de résilience en matière de cybersécurité au sein de l'UE.

La directive *NIS 2* devrait être transposée par chaque état membre de l'UE en droit national, au plus tard en octobre 2024.En France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), l'autorité nationale en matière de cybersécurité et de cyberdéfense, assure ensuite en tant que régulateur le respect de la loi nationale, en ayant recours, si nécessaire, à des sanctions administratives sévères et à des mesures correctives.

Résilience de l'UE : le Conseil adopte une directive visant à renforcer la résilience des entités critiques

Le Conseil a adopté le 14 décembre 2022 une directive et une recommandation qui visent à réduire les vulnérabilités et à renforcer la résilience des entités critiques.

Les entités critiques sont des entités qui fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, la santé et la sécurité publiques ainsi que l'environnement. Elles doivent être en mesure de prévenir les attaques hybrides, les catastrophes naturelles, les menaces terroristes et les urgences de santé publique, ainsi que de s'en protéger, d'y réagir, d'y faire face et de s'en remettre.

La **directive** adoptée couvre des entités critiques dans un certain nombre de secteurs, tels que l'énergie, les transports, la santé, l'eau potable, les eaux usées et l'espace. Certaines administrations publiques centrales seront également couvertes par certaines dispositions du projet de directive.

Les États membres devront disposer d'une stratégie nationale pour renforcer la résilience des entités critiques, procéder à une évaluation des risques au moins tous les quatre ans et recenser les entités critiques qui fournissent des services essentiels. Les entités critiques devront détecter les risques pertinents susceptibles de perturber considérablement la fourniture des services essentiels, prendre des mesures appropriées pour assurer leur résilience et notifier les incidents perturbateurs aux autorités compétentes.

La directive établit également des règles pour le recensement des entités critiques revêtant une importance européenne particulière. Une entité critique est considérée comme revêtant une importance européenne particulière si elle fournit un service essentiel à six États membres ou plus. Dans ce cas, la Commission peut être invitée par les États membres à organiser une mission de conseil ou peut elle-même proposer, avec l'accord de l'État membre concerné, d'évaluer les mesures mises en place par l'entité concernée pour respecter les obligations découlant de la directive.

La recommandation couvre trois domaines prioritaires : la préparation, la réaction et la coopération internationale. Elle invite les États membres à mettre à jour leur évaluation des risques afin de tenir compte des menaces actuelles et les encourage à effectuer des tests de résistance sur les entités qui exploitent des infrastructures critiques, en accordant la priorité au secteur de l'énergie. Elle invite également les États membres à élaborer, en coopération avec la Commission, un schéma directeur pour une réponse coordonnée en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable. L'UE apportera son soutien aux pays partenaires en vue de renforcer leur résilience et la coopération avec l'OTAN dans ce domaine.

Cybersecurity Act : règlement européen « *Cybersecurity Act* » relatif à l'*ENISA* et à la certification de cybersécurité des technologies de l'information et des communications

Adopté par le Parlement européen le 12 mars puis par le Conseil de l'Union européenne le 17 avril 2019, le règlement européen *Cybersecurity Act* (UE 2019/881) a été publié le 7 juin 2019 et marque une véritable avancée pour l'autonomie stratégique européenne. Il poursuit un double objectif :

- Adoption d'un mandat permanent pour l'*ENISA (European Network and Information Security Agency)*, l'Agence de l'Union européenne pour la cybersécurité, valorisant et développant son rôle de facilitateur des échanges entre les États membres.
- Définition d'un cadre de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification, au sein duquel l'*ENISA* trouve toute sa place. Les certificats délivrés bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne (UE).

Le *Cybersecurity Act* est un acte juridique européen, de portée générale, obligatoire dans toutes ses dispositions. Les États membres sont donc tenus d'appliquer ces dernières telles qu'elles sont définies par le règlement.

Il s'agit d'un règlement d'application directe. Les États membres doivent avoir mis leur organisation nationale en conformité avec les dispositions du règlement dans les deux années suivant sa publication.

Les schémas de certification qui sont publiés par la Commission européenne sont d'application volontaire.

Le règlement concerne les **fabricants et fournisseurs** de produits, services et processus des technologies de l'information et de la communication (TIC) pour leur donner un ensemble d'exigences de sécurité.

Il concerne également les **organismes d'évaluation de la conformité** pour délivrer des certificats de cybersécurité européens en utilisant des méthodes d'évaluation robustes et harmonisées.

Il concerne finalement les **utilisateurs finaux et donneurs d'ordre** afin de leur permettre d'utiliser et choisir des produits TIC, services TIC et processus TIC correspondant à leur besoin de sécurité.

Digitalisation et utilisation de l'IA dans la finance

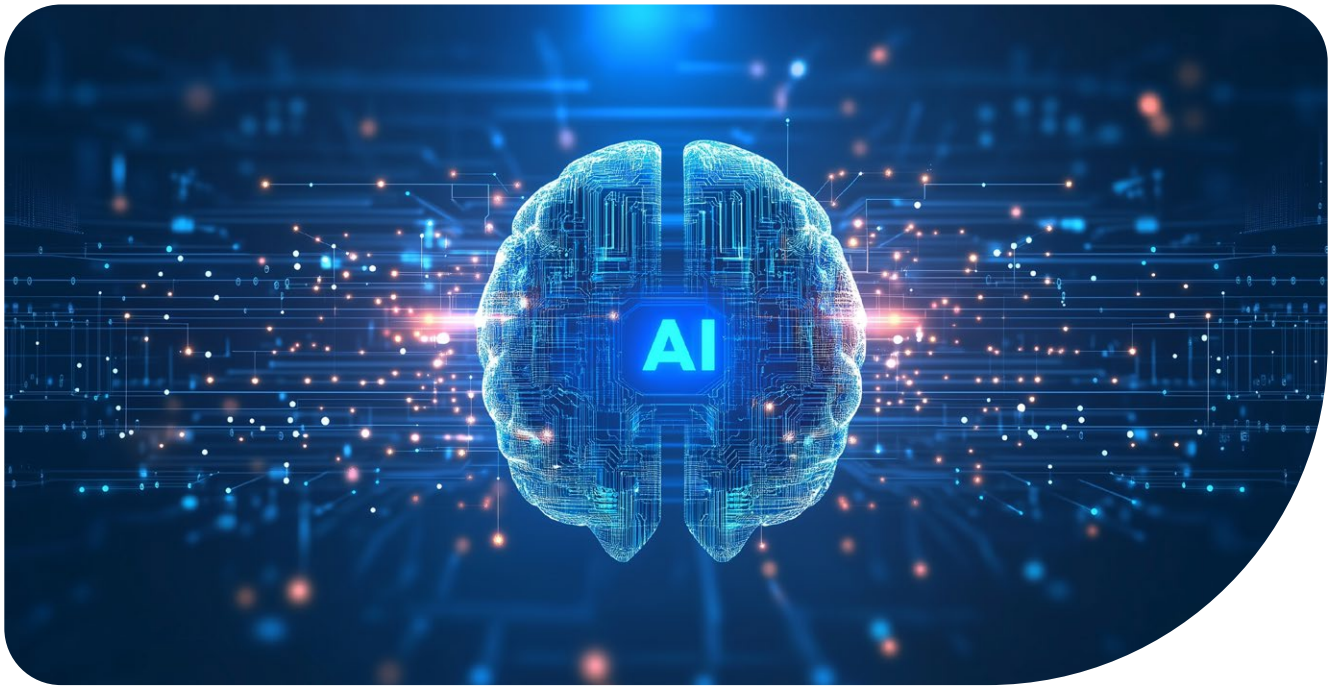
La DSP3 est un ensemble de règles pour le secteur des services de paiement publié par la Commission européenne qui s'appuie sur ses directives précédentes, la DSP2 (publiée en 2015) et la DSP1 (publiée en 2007).

Les directives sur les services de paiement de la Commission européenne ont pour objectif de protéger les consommateurs et de favoriser un marché des paiements plus sûr, plus intégré, plus compétitif et plus efficace au sein de l'UE.

La DSP3 développe le cadre de la DSP2, en particulier dans les domaines de la prévention de la fraude, de la banque ouverte, de l'accès aux données, des droits des consommateurs, de la disponibilité des liquidités et de la concurrence loyale.

Les principales nouveautés introduites par la DSP3 sont :

- Exigences renforcées pour le SCA (**Authentification forte du client** - Prévention de la fraude par usurpation d'identité),
- Concurrence loyale pour les prestataires de services de paiement non bancaires,
- Amélioration de l'open *banking*,
- Des droits plus étendus pour les consommateurs :
  - Amélioration de la communication et de la clarté concernant les frais de conversion de devises ;
  - Des informations plus claires sur le bénéficiaire dans les relevés de compte de paiement ;
  - Plus de transparence sur les frais liés aux distributeurs automatiques de billets ;
  - Une protection accrue des fonds temporairement détenus ou « bloqués ».
- Davantage d'argent liquide disponible :
  - Le « *cashback* » sans achat dans les magasins traditionnels ;
  - Davantage de guichets automatiques.



Règlement européen sur les crypto-actifs (MiCA)

Le règlement (UE) 2023/1114 établit des règles uniformes pour les émetteurs de crypto-actifs qui n'ont pas été réglementés par d'autres actes de l'Union européenne (UE) relatifs aux services financiers et pour les prestataires de services liés à ces crypto-actifs (prestataires de services sur crypto-actifs).

Les règles couvrent :

- Les exigences de transparence et d'information pour l'émission, l'offre au public et l'admission à la négociation de crypto-actifs sur une plate-forme de négociation,
- L'agrément et la surveillance des prestataires de services sur crypto-actifs, des émetteurs de jetons se référant à un ou des actifs et des émetteurs de jetons de monnaie électronique,
- Le fonctionnement, l'organisation et la gouvernance des émetteurs et des prestataires de services sur crypto-actifs,
- La protection des détenteurs de crypto-actifs et des clients des prestataires de services,
- Les mesures visant à prévenir les opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché.

Le règlement s'applique à l'émission, à l'offre au public, à l'admission à la négociation de crypto-actifs, et à la prestation de services liés aux crypto-actifs.

Il distingue les types de crypto-actifs suivants :

- Les **jetons de monnaie électronique** (crypto-actifs qui stabilisent leur valeur par rapport à une monnaie officielle unique),
- Les **jetons se référant à un ou des actifs** (crypto-actifs qui stabilisent leur valeur par rapport à d'autres actifs ou à un panier d'actifs),
- Les crypto-actifs autres que les jetons se référant à un ou des actifs ou les jetons de monnaie électronique.

Les offreurs ou les personnes qui demandent l'admission à la négociation de crypto-actifs autres que les jetons se référant à un ou des actifs et les jetons de monnaie électronique doivent :

- Être une personne morale,
- Publier un livre blanc sur les crypto-actifs et toute communication commerciale sur leur site internet,
- Agir d'une manière honnête, loyale et professionnelle,
- Communiquer avec les détenteurs et les détenteurs potentiels de crypto-actifs de manière loyale, claire et non trompeuse,
- Détecter, prévenir, gérer et communiquer tout conflit d'intérêts,
- Être tenus responsables des dommages occasionnés par des informations erronées dans le livre blanc,
- Proposer un droit de rétractation aux détenteurs de crypto-actifs.

Les émetteurs de jetons se référant à un ou des actifs qui les proposent au public ou demandent l'admission à la négociation sur une plate-forme de négociation de crypto-actifs doivent :

- Être une personne morale ou une certaine entreprise basée dans l'UE,
- Avoir un agrément de leur État membre de l'UE d'origine,
- Être un établissement de crédit qui produit un livre blanc sur les crypto-actifs approuvé par l'autorité nationale compétente,
- Rembourser, à tout moment, leurs jetons se référant à un ou des actifs sur demande des détenteurs à la valeur marchande des actifs de référence ou en livrant les actifs de référence,
- Publier un livre blanc sur les crypto-actifs et toute communication commerciale sur leur site internet et être tenus responsables des dommages occasionnés par des informations erronées dans le livre blanc,
- Agir d'une manière honnête, loyale et professionnelle,
- Communiquer avec les détenteurs et les détenteurs potentiels de jetons de manière loyale, claire et non trompeuse,
- Agir au mieux des intérêts des détenteurs de jetons et les traiter sur un pied d'égalité,
- Établir et maintenir des procédures efficaces et transparentes pour le traitement rapide, équitable et cohérent des réclamations,
- Détecter, prévenir, gérer et communiquer tout conflit d'intérêts,
- Maintenir à tout moment une réserve d'actifs couvrant les engagements envers les détenteurs de jetons et disposer de fonds propres d'un montant au moins égal au plus élevé des montants suivants :
  - 350 000 EUR ;
  - 2 % du montant moyen de la réserve d'actifs ;
  - Un quart des frais généraux fixes de l'année précédente.
- Établir des plans de redressement et de remboursement s'ils ne sont pas en mesure d'exécuter leurs obligations.

Les émetteurs de jetons de monnaie électronique qui les proposent au public ou demandent leur admission à la négociation sur une plate-forme de négociation de crypto-actifs doivent :

- Être agréés en tant qu'établissement de crédit ou de monnaie électronique,
- Publier un livre blanc sur les crypto-actifs et toute communication commerciale sur leur site internet et être tenus responsables des dommages occasionnés par des informations erronées dans le livre blanc,
- Respecter les règles en matière d'émission, de remboursement et de commercialisation,
- Émettre les jetons au pair à la remise des fonds,
- Rembourser les jetons sur demande du détenteur à tout moment et au pair,
- Investir dans la même monnaie les fonds qu'ils reçoivent dans des actifs sûrs et à faible risque et les déposer sur un compte distinct dans un établissement de crédit,
- Établir des plans de redressement et de remboursement s'ils ne sont pas en mesure d'exécuter leurs obligations.

L'Autorité bancaire européenne (ABE) classe les jetons se référant à un ou des actifs et les jetons de monnaie électronique comme « d'importance significative » si certains critères sont remplis, comme leurs détenteurs, leur valeur ou leurs transferts qui dépassent certains niveaux. Dans ces cas, les émetteurs de tels jetons se référant à un ou des actifs et de jetons de monnaie électronique d'importance significative sont soumis à des exigences supplémentaires, et l'ABE exerce le rôle de surveillance.

Les prestataires de services sur crypto-actifs doivent être :

- Une personne morale ou certaines entreprises agréées par leur autorité nationale en tant que prestataire de services sur crypto-actifs, ayant un siège statutaire dans un État membre où elles fournissent au moins une partie de leurs services, une direction effective et au moins un des administrateurs résidant dans l'UE ; ou
- Sous certaines conditions, un établissement de crédit, un dépositaire central de titres, une entreprise d'investissement, un opérateur de marché, un établissement de monnaie électronique, une société de gestion des organismes de placement collectif en valeurs mobilières ou de fonds d'investissement alternatifs.

Tous les prestataires de services sur crypto-actifs ont les obligations suivantes :

- Agir de manière honnête, loyale et professionnelle au mieux des intérêts réels et potentiels des clients,
- Fournir aux clients des informations loyales, claires et non trompeuses,
- Ne pas induire les clients en erreur, que ce soit délibérément ou par négligence, quant aux avantages réels ou supposés des crypto-actifs, et les avertir des risques encourus,
- Mettre leur politique en matière de tarification, de coûts et de frais et les incidences sur le climat et l'environnement de chaque crypto-actif à disposition du public de manière visible sur leur site internet,
- Mettre en place des garanties prudentielles d'un montant au moins égal au plus élevé des montants suivants :
  - Les exigences de capital minimal permanent indiquées à l'annexe IV ; ou
  - Un quart des frais généraux fixes de l'année précédente.
- Veiller à ce que les membres de l'organe de direction jouissent d'une honorabilité suffisante et possèdent les connaissances, l'expérience, les compétences et le temps nécessaires à l'exercice effectif de leurs fonctions,
- Mettre en œuvre des politiques et des procédures visant à prévenir le blanchiment de capitaux, le financement du terrorisme ou d'autres infractions,
- Maintenir les crypto-actifs et les fonds des clients séparés des autres actifs et ne pas les utiliser pour leur propre compte,
- Établir et maintenir des procédures efficaces et transparentes pour traiter les réclamations des clients de manière rapide, équitable et cohérente,
- Maintenir et mettre en œuvre une politique efficace pour détecter, prévenir, gérer et communiquer les conflits d'intérêts,
- Prendre toutes les mesures raisonnables pour éviter tout risque lors de l'externalisation des activités,
- Concevoir, si nécessaire, un plan pour la liquidation ordonnée de leurs activités.

Des règles spécifiques couvrent :

- Les rachats des émetteurs de jetons se référant à un ou des actifs et des prestataires de services sur cryptoactifs,
- Des mesures de prévention et d'interdiction des abus de marché, comme les opérations d'initiés et l'utilisation abusive d'informations privilégiées,
- Les pouvoirs et les rôles des autorités nationales, de l'ABE et de l'Autorité européenne des marchés financiers (AEMF).

Le règlement ne s'applique pas :

- Aux crypto-actifs qui sont couverts par d'autres actes de l'UE relatifs aux services financiers (notamment ceux qui sont considérés comme des instruments financiers, des pensions ou des produits d'assurance),
- Aux prestataires de services sur crypto-actifs exclusivement pour leurs entreprises mères ou filiales, les liquidateurs et les administrateurs agissant dans le cadre de procédures d'insolvabilité,
- A la Banque centrale européenne et aux banques centrales nationales, à la Banque européenne d'investissement, au mécanisme européen de stabilisation financière, au mécanisme européen de stabilité et aux organisations internationales publiques,
- Aux crypto-actifs exclusifs et non interchangeables avec d'autres.

La Commission européenne présente au Parlement européen et au Conseil de l'Union européenne aux différentes étapes suivant l'entrée en vigueur du règlement, un rapport sur :

- Les dernières évolutions en matière de crypto-actifs (après 18 mois),
- L'évaluation intermédiaire du règlement (après 24 mois),
- L'application du règlement (après 48 mois).

La Commission a également le pouvoir d'adopter des actes délégués et des actes d'exécution.

L'AEMF, en coopération avec l'ABE, soumet au Parlement et au Conseil un **rapport** public, 12 mois après l'entrée en vigueur du règlement, puis tous les ans, sur l'application de la législation et l'évolution des marchés de crypto-actifs.

Le règlement s'applique à partir du 30 décembre 2024. Toutefois, les règles relatives aux jetons se référant à un ou des actifs (titre III) et aux jetons de monnaie électronique (titre IV) s'appliquent depuis le 30 juin 2024.

Contact

Agnès de RIBET

Associée,
en charge du *Business Development*,
du *Marketing* et de la Communication

T +33 (0)1 41 25 85 85
M agnes.deribet@fr.gt.com

C.C.L.A.I.R.E **Piliers d'une stratégie ambitieuse, la réaffirmation de nos valeurs s'inscrit dans un schéma mondial : Courage, Collaboration, *Leadership*, Agilité, Intégrité, Respect, Excellence.**

Grant Thornton

grantthornton.fr